From: ISS World Seminars
To: Cindy London
Subject: Successful Use of Online Social Networking for Cyber Crime Investigation and Intelligence Gathering
Date: Friday, September 28, 2018 7:29:20 AM

Presented by:

Charles Cohen, **Cohen Training and Consulting, LLC**
[Charles Cohen also holds the position of Captain, Cyber Crimes and Investigative Technologies Section, **Indiana State Police**]

TeleStrategies Logo

AGENDA

This two day (16 hour) course is designed for private and public sector investigators and analysts. Students with any level of familiarity with the Internet and computers, from beginning to advanced, will find this course beneficial.

The program gives students an up-to-date understanding of how social networking sites work and how members act and interact. Student will learn what information is available on various sites and how to integrate that information into criminal investigations and criminal intelligence analysis.

Session #1: Online Social Media: Tools, Tricks, and Techniques

Too often, investigators and analysts overlook or underutilize this valuable resource. Social networking sites are virtual communities. As in any large community, criminal organizations, fraud, violet crime, and victimization exist. Investigators need to understand these communities along with the tools, tricks, and techniques to prevent, track, and solve crimes.

Current trends include social networks based around live streaming video, like TinyChat and SnapChat, and mobile social networks like, Foursquare, Vibe, and Vine. These emergent technologies lead to risks and opportunities for law enforcement professionals that never previously existed. Current and future undercover officers must now face a world in which facial recognition and Internet caching make it possible to locate an online image posted years or decades before. The meshing of geolocation, metadata exploitation, social networking, and mobile devices allow officers to employ

new investigative techniques not previously available.

Session #2: Facebook: Information Exploited

While there are over 1,000 social networking sites on the Internet, Facebook is by far the most populous, with over 1.1 billion profiles. It has a larger population as the US and UK combined, making it the third largest country by population. There are over 350 million images and 190 million status updates loaded on Facebook every day. This session will cover topics including Facebook security and account settings, Facebook data retention and interaction with law enforcement, and common fraud schemes involving Facebook. Recent additions and changes to Facebook, such as the Poke application for iOS devices, Graph Search, and Archive, make is more important than ever for investigators and analysts to fully understand this community.

Session #3: OSINT: Observation & Infiltration

Open source intelligence (OSINT) is a form of intelligence collection that involves finding, selecting, and acquiring information from publicly available sources and then analyzing it to produce actionable intelligence. Now that the Internet is dominated by Online Social Media, OSINT is a critical component of both criminal and national security investigations. Too often, investigators and analysts overlook or underutilize this valuable resource.

Attendees will explore the challenges that analysts and investigators face differentiating between observation and infiltration of predicated chatter. The advantages and disadvantages of various methods to conceal identities while engaging in online observation and infiltration will be discussed.

Session #4: Counterintelligence & Liabilities Involving Online Social Media

Current and future undercover officers must now face a world in which facial recognition and Internet caching make it possible to locate an online image posted years or decades before. The meshing of geolocation, social networking, and mobile devices allow officers to employ new investigative techniques not previously available. There are risks posed to those in the public arena, and those charged with protecting them, associated with online social media and online social networking. The online social networking activities of employees, along with ever-increasing availability of information in the online public domain, present real challenges to companies and governments.

Session #5: What Investigators Need to Know about Hiding on the Internet

Criminal investigators and analysts need to understand how people conceal their identity on the Internet. Technology may be neutral, but the ability to hide ones identity and location on the Internet can be both a challenge and an opportunity. Various methods of hiding ones identity and location while engaged in activates on the Internet, provides an opportunity for investigators to engage in covert online research while also providing a means for criminals to engage in surreptitious communication in furtherance of nefarious activities. As technologies, such as digital device fingerprinting, emerge as ways to attribute identity this becomes a topic about which every

investigator and analyst must become familiar.

Students receive course material, including legal process contact information, preservation letters, boilerplate compliance documents, and resource guides.

NOTICE: Course contains graphic content including profanity, and sexual and violent images.

ABOUT THE INSTRUCTOR

Chuck Cohen's formal education includes a Master of Business Administration from Indiana Wesleyan University and an undergraduate degree from Indiana University with a double major in Criminal Justice and Psychology. Chuck is also a Certified Fraud Examiner.

He is a Lieutenant serving the Indiana State Police, where he has been employed since 1994. He is currently the Commander, Cybercrime and Investigative Technologies Section. In this capacity, Lt. Cohen is responsible for the cybercrime, electronic surveillance, technical services, and Internet crimes against children units along with overseeing the department's overt and covert criminal intelligence function. Chuck is the Indiana Internet Crimes Against Children (ICAC) Task Force Commander.

Chuck speaks internationally on topics including the implications of online social networks in criminal investigations and criminal intelligence gathering, cybercrime, online fraud, money laundering, corruption investigations, and the investigation of skilled criminal offenders. He is an Adjunct Instructor at Indiana University Bloomington, where he teaches Foundations of Criminal Investigation.

Chuck was a member of the Office of the Director of National Intelligence Summer Hard Problem Program in 2008, 2009, and 2010. The 2008 the study topic was "3D Cyber Space Spillover: Where Virtual Worlds Get Real." The 2009 topic was "Mixed Reality: When Virtual Plus Real Equals One." And, in 2010, the topic was "Online Social Media."

He is a published author, including peer-reviewed material and a cover article for Police Chief Magazine. Chuck was recently featured on the cover of the National White Collar Crime Center's Informant magazine and a feature guest on the syndicated radio program "The Badge" on SiriusXM. He was a subject matter expert for a Fox nationally syndicated show regarding criminal activity in online dating sites and for the Canadian Broadcasting Corporation's national news regarding criminal activity in Virtual Worlds.

Complete Seminar Agenda and Registration

To review the full seminar agenda, or to register online, please click here.

If you do not wish to receive future emails from ISS World Seminars, click here to opt-out .

TeleStrategies, Inc | 6845 Elm Street, Suite 310 | McLean | VA | 22101 | US